

FOOLING SETS (A.K.A. CROSS-FREE MATCHINGS) AND RANK IN NON-ZERO CHARACTERISTIC

MIRJAM FRIESEN AND DIRK OLIVER THEIS

ABSTRACT. In a bipartite graph, a *cross-free matching* or *fooling set* is a matching no two of whose edges induce a C_4 . Dietzfelbinger, Hromkovič, and Schnitger (1994) showed that the maximum cardinality of a cross-free matching is at most the square of the rank of the bipartite adjacency matrix of the graph (regardless of over which field the rank is computed), and asked, whether this bound can be improved.

We show that if the rank is taken in characteristic 2, then the bound is asymptotically tight. For other non-zero characteristic, we show that a stronger form of Dietzfelbinger et al.'s inequality (implicit in their proof) for “weighted” adjacency matrices is tight. We use cyclic matrices defined by a linear recurrence relation.

Keywords: Bipartite matching, cross-free matching, fooling set, minimum rank problems, communication complexity.

1. INTRODUCTION

A *cross-free matching* in a bipartite graph G is a matching in G , no two of whose edges induce a C_4 in G . Let M be a bipartite adjacency matrix of G . A cross-free matching can be considered as a subset F of the index set of M with the following properties:

$$M_{k,\ell} \neq 0 \quad \text{for all } (k, \ell) \in F, \quad (1a)$$

$$M_{k,\ell'} M_{k',\ell} = 0 \quad \text{for all } (k, \ell), (k', \ell') \in F \text{ with } (k, \ell) \neq (k', \ell'). \quad (1b)$$

A subset $F \subset \{1, \dots, m\} \times \{1, \dots, n\}$ of the index set of an $m \times n$ 0/1-matrix M is called a *fooling set* if it satisfies (1). The *size* of a fooling set is its cardinality. Since we are interested in comparing the size of a fooling set / cross-free matching with the rank of the (adjacency) matrix, we will be working with the matrix version of the definition and use the name fooling set. We denote by $\text{fool}(M)$ the largest size of a fooling set in the matrix M .

In graph theory, cross-free matchings are best known as a lower bound on the size of biclique coverings of graphs (e.g. [3, 8]). A biclique covering is a set of bicliques in G such that every edge of G is contained in at least one of the bicliques. It is easily verified that the minimum number of bicliques needed to cover all edges of G is at most the maximum size of a cross-free matching in G , with equality for some classes of bipartite graphs [3, 15].

In computational complexity, fooling sets provide lower bounds for the communication complexity of Boolean functions (see, e.g., [1, 12, 14, 4, 10]), and for the number of states of an automaton accepting a given language (e.g., [7]).

In matrix theory, fooling sets are known (under a different name, e.g. [2, Lemma 2.4]) as a lower bound to the so-called nonnegative rank of a nonnegative matrix over a semiring.

In polytope theory, given a polytope P , fooling sets are a lower bound to the number of facets of any polytope Q which can be mapped onto P by a projective mapping. Similarly, in combinatorial optimization, fooling sets are lower bounds to the minimum sizes of Linear Programs for combinatorial optimization problems [16, 9]. For example, it is an open question whether Edmond's matching polytope for a complete graph on n vertices admits a fooling set whose size grows quicker in n than the dimension of the polytope. Such a fooling set would yield a fairly spectacular improvement on the currently known lower bounds of sizes of Linear Programming formulations for the matching problem. (The matching polytope has not yet profited from other lower bounding strategies recently used for some types of polytopes [6].) See [5] for bounds based on fooling sets for a number of combinatorial optimization problems, including Bipartite Matching.

In each of the areas where cross-free matchings / fooling sets are used as lower bounds, upon embarking on a search for large fooling sets in a complicated matrix, one is interested in *a priori* upper bounds on their sizes. A theorem of Dietzfelbinger et al. ([4, Thm. 1.4]¹, or see [12, Lemma 4.15]) gives such an upper bound in terms of the rank of the matrix. They prove² that, for every field \mathbb{k} and every 0/1-matrix M

$$\text{fool}(M) \leq \min\{(\text{rk}_{\mathbb{k}} S)^2 \mid \text{supp } S = \text{supp } M\} \quad (2a)$$

holds, where $\text{supp } S := \{(k, \ell) \mid S_{k,\ell} \neq 0\}$ is the support of the matrix. In particular

$$\text{fool}(M) \leq (\text{rk}_{\mathbb{k}} M)^2. \quad (2b)$$

It is an open question whether these inequalities can be improved or not. Dietzfelbinger et al. [4, Open Problem 2] specifically asked this question regarding (2b). Currently, the best known examples of 0/1-matrices (attributed to M. Hühne in [4]) are such that $\text{fool}(M) = (\text{rk}_{\mathbb{Q}} M)^{\log_4 6}$ ($\log_4 6 = 1.292 \dots$); for the stronger inequality (2a), Klauck and de Wolf [10] have examples with $\text{fool}(M) = (\text{rk}_{\mathbb{Q}} S)^{\log_3 6}$ ($\log_3 6 = 1.63 \dots$).

In this paper, we deal with Dietzfelbinger et al.'s open problem in the case of fields \mathbb{k} of non-zero characteristic p . For a prime number p , we denote by \mathbb{F}_p the finite field with p elements. We will prove the following.

Theorem 1. *For every prime number p , there is a family of matrices $(S^{(t)})_{t=1,2,3,\dots}$ over \mathbb{F}_p with $\text{rk}_{\mathbb{F}_p} S^{(t)} \rightarrow \infty$, which have the property*

$$\text{fool}(M^{(t)}) / (\text{rk}_{\mathbb{F}_p} S^{(t)})^2 \longrightarrow 1,$$

where $M^{(t)}$ denotes the 0/1-matrix with the same support as $S^{(t)}$. Hence, inequality (2a) is tight if the characteristic of \mathbb{k} is non-zero.

¹In [4], theorem is stated in terms of the maximum of $\text{fool}(M)$ and $\text{fool}(J - M)$, for J the all-1s-matrix, to make it directly applicable as a lower bound in communication complexity. Their proof proceeds by establishing inequality (2b). Note that the difference between $\text{rk}(M)$ and $\text{rk}(J - M)$ is at most 1.

²Strictly speaking, [4] only proves (2b), but the proof goes through word for word to show (2a).

We emphasize that, in the case of characteristic $p > 0$, not only is the exponent 2 on the rank in equation (2a) best possible, but so is the constant 1 in front of the rank.

The most important case is $p = 2$. Here, [4, Thm 1.3] proves that while a constant fraction of $n \times n$ matrices have rank n , the fraction of those matrices which have a fooling set of size larger than $\Omega(\log n)$ tends to zero with $n \rightarrow \infty$. Theorem 1 implies the following.

Corollary 2. *Inequality (2b) is tight if the characteristic of \mathbb{k} is 2.* \square

The remainder of this paper is organized as follows. In the next section, we describe our construction of matrices and prove some easy facts about it. The more difficult parts of the argument are done in Section 3. We conclude the paper with a discussion of open problems.

2. CONSTRUCTION OF THE MATRICES

We now describe the construction of our matrices. Let p be a prime number and $r \geq 2$ an integer. Define the function $f: \mathbb{Z} \rightarrow \mathbb{F}_p$ by the recurrence relation

$$f(k+r) = -f(k) - f(k+1) \quad \text{for all } k \in \mathbb{Z} \quad (3a)$$

and the initial conditions

$$f(0) = 1, \text{ and } f(1) = \dots = f(r-1) = 0. \quad (3b)$$

Fix an integer $n > r$. From the sequence, we define an $(n \times n)$ -matrix as follows. For ease of notation, the matrix indices are taken to be in $\{0, \dots, n-1\} \times \{0, \dots, n-1\}$. We let

$$S_{k,\ell} = f(k-\ell). \quad (4)$$

We will prove that $\text{rk } S \leq r$ and that the set

$$F := \{(j, j) \mid j = 0, \dots, n-1\} \quad (5)$$

is a fooling set in S under some additional conditions on r and n . Strictly speaking, we ought to talk about the fooling set property in the 0/1-matrix M with the same support as S . We will ignore this subtlety here for the sake of brevity.

The more difficult part of the argument, Lemma 2.3, is proved in the next section. In this section, we will only give the details for the easy Lemmas 2.1 (rank) and 2.2 (fooling set property), which together with Lemma 2.3 imply Theorem 1. We start with the estimate for the rank.

Lemma 2.1. *The rank of S is at most r .*

Proof. From (3a), for $k \geq r$, we deduce the equation $S_{k,\cdot} = -S_{k-r,\cdot} - S_{k-r+1,\cdot}$. Hence, each of the rows $S_{k,\cdot}$, $k \geq r$, is a linear combination of the first r rows of S . \square

Remark. It can be seen that the rank is, in fact, equal to r : The top-left $r \times r$ sub-matrix is regular because it is upper-triangular with non-zeros along the diagonal.

The following lemma reduces the fooling set property (1b) to a property of the function f .

Lemma 2.2. *If*

$$f(k)f(-k) = 0 \quad \text{for all } k \in \{1, \dots, n-1\} \quad (6)$$

then the set F defined in (5) is a fooling set in S .

Proof. It is clear from (3b) and (4) that $S_{j,j} = f(0) = 1$ for all $j = 0, \dots, n-1$, so it remains to verify (1b). Since

$$S_{i,j}S_{j,i} = f(i-j)f(j-i) = f(i-j)f(-(i-j)),$$

if $f(k)f(-k) = 0$ for all $k = 1, \dots, n-1$, then $S_{i,j}S_{j,i}$ is zero whenever $i \neq j$. This proves (1b). \square

In the next section we will prove the following.

Lemma 2.3. *For all integers $t \geq 1$, if we let $r := p^t + 1$ and $n := r(r-1) + 1$, then $f(k)f(-k) = 0$ for all $k \in \mathbb{Z} \setminus n\mathbb{Z}$.*

Now all ingredients are ready to prove Theorem 1.

Proof of Theorem 1. Let p be a prime number. For every integer $t \geq 1$, let $r := p^t + 1$ and $n := r(r-1) + 1$, and define the matrix $S^{(t)} := S$ over \mathbb{F}_p as in (4). Let M be the $n \times n$ 0/1-matrix with the same support as S . By Lemma 2.1, the rank of $S^{(t)}$ is at most r , and from Lemmas 2.2 and 2.3 we conclude that $S^{(t)}$ contains a fooling set of size n . Hence, we have

$$1 \geq \frac{\text{fool}(S^{(t)})}{\text{rk}_{\mathbb{F}_p}(S^{(t)})^2} \geq \frac{r^2 - r + 1}{r^2} \geq 1 - p^{-t}/4 \xrightarrow{t \rightarrow \infty} 1,$$

where the left-most inequality is from (2a). (That $\text{rk}_{\mathbb{F}_p} S^{(t)} \rightarrow \infty$ follows either from Remark 2.1 or from (2a).) \square

3. PROOF OF LEMMA 2.3

In this section let f be defined as in (3). The proof of Lemma 2.3 is done in three parts. We first prove a statement about blocks of zeros in $f(0), \dots, f(n-1)$. This allows us to show that, for r and n as in Lemma 2.3, the function f is n -periodic. (Recall that a function g on \mathbb{Z} is called n -periodic if $g(k+n) = g(k)$ for all $k \in \mathbb{Z}$.) Thirdly, we combine these two results for the proof of Lemma 2.3.

The first lemma states that in every section $\{jr, \dots, (j+1)r-1\}$, $j = 0, 1, \dots$, there is a block of zeros whose length decreases with j .

Lemma 3.1. *For $j = 0, \dots, r-2$, we have*

$$f(jr+i) = 0 \quad \text{for } i = 1, \dots, r-1-j. \quad (7)$$

Proof. Equation (7) is true for $j = 0$ by (3b). Suppose (7) holds for some $j < r-2$. Then $f((j+1)r+i) = 0$ for $i = 1, \dots, r-1-(j+1)$, because, by (3a),

$$f((j+1)r+i) = f(jr+i+r) = -f(jr+i) - f(jr+(i+1)) = -0 - 0$$

holds. \square

Every function on \mathbb{Z} with values in a finite field which is defined by a (reversible) linear recurrence relation is periodic (cf. e.g. [13]). Here we prove that a specific number n is a period of f as defined in (3).

Lemma 3.2. *If $r = p^t + 1$ for some integer $t \geq 1$, then $n := r(r-1) + 1$ is a period of the function f .*

Proof. In this proof, for convenience, we identify \mathbb{F}_p with the integers modulo p .

Consider $h(j, i) := f((j+1)r - i)$ for $i, j \in \mathbb{Z}$. We have to show that

$$h(r-1, 0) = 0. \quad (8a)$$

$$h(r-1, 1) = \dots = h(r-1, r-2) = 0, \text{ and} \quad (8b)$$

$$h(r-1, r-1) = 1. \quad (8c)$$

We will first prove the following claims.

Claim (a). For all $i, j \in \mathbb{Z}$,

$$h(j+1, i) = -h(j, i) - h(j, i-1).$$

Claim (b). For $j = 0, \dots, r-3$

$$h(j, -1) = 0, \quad h(j, j+1) = 0.$$

Claim (c). For $j = 0, \dots, r-2$ and $0 \leq i \leq j$

$$h(j, i) = (-1)^{j+1} \binom{j}{i} \pmod{p}.$$

Before we prove the claims, we show how they imply (8). Recalling the well-known fact that

$$\binom{p^t}{i} = 0 \pmod{p}$$

for every integer $t \geq 1$ and for all $i = 1, \dots, p^t - 1$ (cf. e.g. [13]), the equations (8b) follow by applying Claims a and c with $j := r-2$: For $i = 1, \dots, r-2 = p^t - 1$, since

$$\begin{aligned} h(r-1, i) &= -h(r-2, i) - h(r-2, i-1) = \\ &= -(-1)^{r-1} \binom{r-2}{i} - (-1)^{r-1} \binom{r-2}{i-1} \pmod{p}, \end{aligned}$$

it follows that

$$\begin{aligned} h(r-1, i) &= -\binom{r-1}{i} \pmod{p} \\ &= -\binom{p^t}{i} \pmod{p} \\ &= 0 \pmod{p}. \end{aligned}$$

To prove (8c), we infer from the claims that

$$\begin{aligned} h(r-1, r-1) &= -h(r-2, r-1) - h(r-2, r-2) = \\ &= -f((r-1)r - r + 1) - (-1)^{r-1} \binom{r-2}{r-2} = \\ &= -f((r-2)r + 1) - (-1)^p = 1, \end{aligned}$$

where the last equation follows from Lemma 3.1 and the fact that $-(-1)^p = 1$ even for $p = 2$. Finally, for (8a), we conclude that

$$\begin{aligned} h(r-1, 0) &= -h(r-2, 0) - h(r-2, -1) = \\ &= -(-1)^{r-1} \binom{r-2}{0} - f(r^2 - (r-1)) = -(-1)^p - h(r-1, r-1) = \\ &= -(-1)^p - 1 = 0, \end{aligned}$$

where the last-but-one equation follows from (8c).

Proof of Claim (a). This is a straightforward computation. For all j, i , we compute

$$\begin{aligned} h(j+1, i) &= f((j+2)r - i) = \\ &= f((j+1)r - i + r) = -f((j+1)r - i) - f((j+1)r - (i-1)) = \\ &= -h(j, i) - h(j, i-1). \end{aligned}$$

□

Proof of Claim (b). This claim follows from Lemma 3.1. We have

$$h(j, -1) = f((j+1)r + 1) = 0 \quad \text{for } j = 0, \dots, r-3,$$

and

$$h(j, j+1) = f((j+1)r - j - 1) = f(jr + r - 1 - j) = 0 \quad \text{for } j = 0, \dots, r-2.$$

□

Proof of Claim (c). Since $h(0, 0) = -1$, Claim (c), follows from Claims (a) and (b). □

This completes the proof of Lemma 3.2. □

Combining Lemmas 3.1 and 3.2 allows us to finish the proof of Lemma 2.3.

Proof of Lemma 2.3. We need to show $f(k)f(-k) = 0$ whenever $n \nmid k$. By Lemma 3.2, this is equivalent to showing $f(k)f(n-k) = 0$ for $k = 1, \dots, n-1$. Given such a k , let j, i be such that $k = jr + i$ and $0 \leq i \leq r-1$.

If $i \leq r-1-j$, then $f(k) = 0$ by Lemma 3.1, and we are done. If, on the other hand, $i > r-1-j$, then

$$n - k = r^2 - r + 1 - jr - i = (r-1-(j+1))r + (r-i+1),$$

and $r-i+1 \leq j+1$, so, by Lemma 3.1, we have $f(n-k) = 0$. □

4. CONCLUSION

Dietzfelbinger et al.'s original question regarding inequality (2b) remains open in characteristic $p \neq 2$. There, it may be possible that (2b) is not tight although our theorem shows that (2a) is. In particular, for characteristic zero, Klauck and de Wolf [10] have given examples of fooling sets of size 6^k together with $\{0, \pm 1\}$ -matrices of rank 3^k with the same support ($k = 1, 2, 3, \dots$). Thus, the exponent on the rank in inequality (2a) with $\mathbb{k} := \mathbb{Q}$ must be at least $\log_3 6 = 1.63\dots$, while the best known bound for inequality (2b) is $\log_4 6 = 1.292\dots$.

Moreover, in characteristic zero, given M , the minimum possible $\text{rk } S$ on the right hand side of inequality (2a) may depend not only on the characteristic, but on the field \mathbb{k} itself. Indeed, there are examples of matrices M for which the minimum on the right hand side of (2a) differs between $\mathbb{k} = \mathbb{Q}$ and $\mathbb{k} = \mathbb{R}$, see e.g. [11]. Hence, for characteristic zero, we ask the following weaker version of Dietzfelbinger et al.'s question.

Question 4.1. *Is there a field \mathbb{k} (of characteristic zero) over which the fooling set vs. rank inequality in (2a) can be improved?*

We believe that our approach of using cyclic matrices, together with the known results about the spectral theory of these matrices, can be used to show the tightness of inequality (2a) for some fields of characteristic zero (ongoing work).

As mentioned in the introduction, another problem in characteristic zero comes from polytope theory. Let P be a polytope. Define the 0/1-matrix $M(P)$, whose rows are indexed by the facets of P and whose columns are indexed by the vertices of P , as follows:

$$M(P)_{F,v} := \begin{cases} 0, & v \in F \\ 1, & v \notin F \end{cases}$$

The following inequality then follows from (2a) (cf. [5]):

$$\text{fool}(M(P)) \leq (\dim P + 1)^2. \quad (9)$$

The following variant of Dietzfelbinger et al.'s question is thus of pertinence in polytope theory and combinatorial optimization.

Question 4.2. *Can the fooling set vs. dimension inequality (9) be improved (for polytopes)?*

To our knowledge, the best known lower bound for the best possible exponent on the dimension in inequality (9) is 1.

REFERENCES

- [1] Sanjeev Arora and Boaz Barak, *Computational complexity*, Cambridge University Press, Cambridge, 2009, A modern approach. MR 2500087 (2010i:68001) [1](#)
- [2] Joel E. Cohen and Uriel G. Rothblum, *Nonnegative ranks, decompositions, and factorizations of nonnegative matrices*, Linear Algebra Appl. **190** (1993), 149–168. MR 1230356 (94i:15015) [2](#)
- [3] Milind Dawande, *A notion of cross-perfect bipartite graphs*, Inform. Process. Lett. **88** (2003), no. 4, 143–147. MR 2009283 (2004g:05118) [1](#)

- [4] Martin Dietzfelbinger, Juraj Hromkovič, and Georg Schnitger, *A comparison of two lower-bound methods for communication complexity*, Theoret. Comput. Sci. **168** (1996), no. 1, 39–51, 19th International Symposium on Mathematical Foundations of Computer Science (Košice, 1994). MR 1424992 (98a:68068) [1](#), [2](#), [3](#)
- [5] Samuel Fiorini, Volker Kaibel, Kanstantin Pashkovich, and Dirk Oliver Theis, *Combinatorial bounds on nonnegative rank and extended formulations*, [arXiv:1111.0444](#) (submitted to *Discrete Math.*), 2012+. [2](#), [7](#)
- [6] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf, *Linear vs. semi-definite extended formulations: Exponential separation and strong lower bounds*, STOC, 2012. [2](#)
- [7] Hermann Gruber and Markus Holzer, *Finding lower bounds for nondeterministic state complexity is hard (extended abstract)*, Developments in language theory, Lecture Notes in Comput. Sci., vol. 4036, Springer, Berlin, 2006, pp. 363–374. MR 2334484 [1](#)
- [8] S. Jukna and A. S. Kulikov, *On covering graphs by complete bipartite subgraphs*, Discrete Math. **309** (2009), no. 10, 3399–3403. MR 2526759 (2010h:05231) [1](#)
- [9] Volker Kaibel, *Extended formulations in Combinatorial Optimization*, Optima – Mathematical Optimization Society Newsletter **85** (2011), 2–7, www.mathopt.org/Optima-Issues/optima85.pdf. [2](#)
- [10] Hartmut Klauck and Ronald de Wolf, *Fooling one-sided quantum protocols*, [arXiv:1204.4619](#), 2012. [1](#), [2](#), [7](#)
- [11] Swastik Kopparty and K. P. S. Bhaskara Rao, *The minimum rank problem: a counterexample*, Linear Algebra Appl. **428** (2008), no. 7, 1761–1765. MR 2388655 (2009a:15002) [7](#)
- [12] Eyal Kushilevitz and Noam Nisan, *Communication complexity*, Cambridge University Press, Cambridge, 1997. MR 1426129 (98c:68074) [1](#), [2](#)
- [13] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994. MR 1294139 (95f:11098) [5](#)
- [14] L. Lovász and M. Saks, *Möbius functions and communication complexity*, Proc. 29th IEEE FOCS, IEEE, 1988, pp. 81–90. [1](#)
- [15] José A. Soto and Claudio Telha, *Jump number of two-directional orthogonal ray graphs*, Integer programming and combinatorial optimization, Lecture Notes in Comput. Sci., vol. 6655, Springer, Heidelberg, 2011, pp. 389–403. MR 2820923 (2012j:05305) [1](#)
- [16] Mihalis Yannakakis, *Expressing combinatorial optimization problems by linear programs*, J. Comput. System Sci. **43** (1991), no. 3, 441–466. MR 1135472 (93a:90054) [2](#)

MIRJAM FRIESEN & DIRK OLIVER THEIS: FACULTY OF MATHEMATICS, OTTO VON GUERICKE UNIVERSITY MAGDEBURG, UNIVERSITÄTSPLATZ 2, 39106 MAGDEBURG, GERMANY
E-mail address: theis@ovgu.de <http://dirkolivertheis.wordpress.com>